FILE
DEC 19 2024
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

Microsoft Corporation,

Plaintiff,

v.

Does 1-10 Operating an Azure Abuse Network,

Defendants.

Case No. 1:24CV-2323

FILED UNDER SEAL

APPLICATION OF MICROSOFT CORPORATION FOR AN EMERGENCY *EX PARTE* ORDER FOR TEMPORARY RESTRAINING ORDER AND RELATED RELIEF

INTRODUCTION

Plaintiff Microsoft Corp. ("Microsoft") moves for emergency *ex parte* relief pursuant to Federal Rule of Civil Procedure 65; the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Digital Millenium Copyright Act (17 U.S.C. § 1201), the Lanham Act (15 U.S.C. §§ 1114, 116, & 1125); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962(c)); the common law, and the All Writs Act (28 U.S.C. § 1651). Microsoft's requested relief is necessary for the investigation, abatement, and remediation of Defendants' use of stolen customer credentials to abuse Microsoft's Azure OpenAI Service and generate harmful images. Because prior notice to Defendants of Microsoft's motion would provide Defendants with an opportunity to destroy, move, conceal, or otherwise make inaccessible certain instrumentalities used to obtain unauthorized access into Microsoft software and computer systems and evidence of their unlawful activities, Microsoft seeks relief *ex parte* and is filing concurrently herewith a motion to seal this action. *See, e.g., Microsoft v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.) (*ex parte* relief in action that was sealed until execution of court's orders).

Defendants are groups of persons, including foreign nationals, doing business in the United States in furtherance of a sophisticated scheme to abuse Microsoft's Azure OpenAI Service. The Azure OpenAI Service is Microsoft's implementation of OpenAI's cutting edge generative Artificial Intelligence ("AI") tools, including OpenAI's GTP-4 large language model and DALL-E image generation software. In the simplest terms, Defendants stole authentication information from legitimate Microsoft customers, created a custom tool set designed to use that stolen information to bypass Microsoft authentication gates and AI content safeguards, and then misused Microsoft's software and computers to create harmful images in violation of Microsoft's policies and technical content filtering measures. In doing so, Defendants have harmed Microsoft, its customers, and the public at large. Accordingly, Microsoft respectfully requests:

> (1) An order directing Defendants, their service providers, and/or those acting in concert therewith to preserve evidence related to, and to turn over control of, the "atism.net" domain used to carry out Defendants' misconduct;
>
> (2) an order enjoining Defendants from further violations of the DMCA, CFAA, Lanham Act, RICO Act, and common law; and
>
> (3) an order directing Defendants to show cause why they should not be preliminarily enjoined from the violations of law described in this motion and Microsoft's Complaint. *Ex parte* relief is essential due to the nature of the conduct at issue.

If Microsoft's requests for relief are granted, Microsoft will first act promptly to secure the "aitism.net" domain and will then serve subpoenas on third party service providers whose infrastructure Defendants have misused. After securing the aitism.net domain and serving necessary subpoenas so that preservation obligations are in place, Microsoft will then act diligently to provide notice to Defendants by serving them with all papers in this action via all known means of contacting them. Microsoft will also act promptly to unseal this action and file public redacted versions of the papers in this case.

STATEMENT OF FACTS

This case is fundamentally about Defendants' intrusions into and misuse of the computers and software that make up Microsoft's Azure Platform. Originally announced in 2008 as Microsoft's new cloud computing operating system, "Windows Azure" was built as an extension of Windows New Technology ("Windows NT") and marked the beginning of Microsoft's Cloud Platform as a Service offering. "Windows Azure" became commercially available in 2010 and after more than a decade of evolution is known today simply as "Azure." Azure consists of a global network of Microsoft computers and datacenters responsible for hosting, running, and managing Microsoft and third-party software products. Lyons Decl. ¶¶ 9-11. Figure 1 below depicts the location of some of Azure's physical infrastructure worldwide.

Fig. 1: Azure Global Datacenters

In addition to the Microsoft-owned resources depicted in Figure 1, customers use their own computing resources and public Internet infrastructure to connect to and use Azure services. Lyons Decl. ¶¶ 9-11.

Most Azure cloud services fall into four broad categories: infrastructure as a service, platform as a service, serverless, and software as a service. These are sometimes called the cloud

computing "stack" because they build on top of one another. The most basic category of cloud services is infrastructure as a service ("IaaS"), which allows customers to rent IT infrastructure like servers, virtual machines, storage, networks, and operating systems on a pay-as-you-go basis. On the other end of the spectrum, Software as a Service ("SaaS") adds software to the equation and enables delivery of software applications over the Internet on demand and typically on a subscription basis. Lyons Decl. ¶¶ 10-11.

Commencing in or around July 2024, Defendants began abusing Microsoft IaaS and SaaS customer credentials to gain unauthorized access to Microsoft computers and software. Defendants then used Microsoft's technology stack to steal access to the Azure OpenAI Service, which is Microsoft's implementation of cutting-edge generative AI tools provided by OpenAI. Defendants used their ill-gained access to the Azure OpenAI Service to generate harmful images that violate Microsoft's policies, contracts, and technological controls.

Microsoft's Access Controlled Azure Platform

Microsoft's Azure Platform is an access-controlled, restricted network of computers used in interstate commerce. Lyons Decl. ¶¶ 9-16. A person or company that wishes to use Azure services must first create an Azure account and user profile. Lyons Decl. ¶ 14. Azure users must provide accurate location, name, and contact information and must agree to the Microsoft Customer Agreement. *Id.* Among other things, the Microsoft Customer Agreement states:

> a) Licenses for Products. Products are licensed and not sold. Upon Microsoft's acceptance of each order and subject to Customer's compliance with this Agreement, Microsoft grants Customer a nonexclusive and limited license to use the Products ordered as provided in this Agreement. These licenses are solely for Customer's own use and business purposes and are nontransferable except as expressly permitted under this Agreement or applicable law.
>
> b) Duration of licenses. Online Services and some Software are licensed on a subscription basis for a specified period of time. Subscriptions expire at the end of the applicable subscription period unless renewed. Some Subscriptions renew

> automatically until canceled. The Subscription term for Online Services that are billed in arrears based on usage is the same as the billing period unless otherwise specified in the Product Terms. Perpetual Software licenses become perpetual upon payment in full.
>
> c) End Users. Customer will control access to, and use of, the Products by End Users and is responsible for any use of the Products that does not comply with this Agreement.

Id.; Exbibit 26. The Microsoft Customer Agreement also includes a "restrictions" section that expressly prohibits several categories of conduct:

> Except as expressly permitted in this Agreement or Product documentation, Customer must not (and is not licensed to):
>
> (i) reverse engineer, decompile, or disassemble any Product or Services Deliverable, or attempt to do so (except where applicable law permits despite this limitation);
>
> (ii) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms;
>
> (iii) work around any technical limitations in a Product or Services Deliverable or restrictions in Product documentation;
>
> (iv) separate and run parts of a Product or Services Deliverable on more than one device;
>
> (v) upgrade or downgrade parts of a Product at different times;
>
> (vi) transfer parts of a Product separately; or
>
> (vii) distribute, sublicense, rent, lease, or lend any Products or Services Deliverables, in whole or in part, or use them to offer hosting services to a third party

Id.; Exhibit 26.

Some Azure services are provided free of charge, but most require payment. Microsoft provides pricing models that let customers pay only for the cloud resources they use. Lyons Decl. ¶¶ 14-15. After agreeing to the Microsoft Customer Agreement, a user wishing to access and use Azure resources and services must authenticate themselves with valid Microsoft-provided credentials. Lyons Decl. ¶16. There are several ways users can authenticate themselves to gain access to Azure services. *Id.* For example, users can authenticate themselves

to Azure using Microsoft Entra ID, which is a cloud-based identity and access management service. *Id.* Another way of authenticating and gaining access to Azure is through use of API Keys. *Id.*[1]

Microsoft's Access Controlled and Copyright Protected Azure OpenAI Service Software

The Azure OpenAI Service provides access to many of OpenAI's generative AI models including versions of OpenAI's GPT and DALL-E models. Lyons Decl. ¶17. The Azure OpenAI Service brings together OpenAI's models and APIs with the security and scalability of the Azure cloud platform. *Id.* Microsoft experts in AI research, policy, and engineering collaborate to develop practical tools and methodologies that support AI security, privacy, safety, and quality and embed them directly into the Azure AI platform. *Id.*

The Azure OpenAI Service is sophisticated software that took creativity and ingenuity to write. Declaration of Rodel Fiñones ("Fiñones Decl.") ¶¶ 5-8. Each individual component was created using the expertise and vast experience of Microsoft engineers, utilizing creative thinking to design and build a robust system. *Id.* The Azure OpenAI Service as it exists today depends on many creative decisions that express choices made by authors who wrote the software for Microsoft. *Id.* The Azure software accessed by Defendants without authorization (the "Azure Middleware") is software written for Microsoft that contains Microsoft copyright notices in source code header files. *Id.* Microsoft considers itself to be the owner of the copyright to Azure Middleware. *Id.*

Azure OpenAI Service is made available to customers under the terms governing their subscriptions to Microsoft Azure Services, including Product Terms for Microsoft Azure Services. Microsoft's Code of Conduct also limits permissible usage of the Azure OpenAI

[1] An application programing interface ("API") is computer code that allows software programs to communicate with each other. An API key is an electronic signature that authenticates the source of an API call.

Service. Lyons Decl. ¶ 18. Microsoft's contractual and policy terms prohibit, for example, content that describes, features, or promotes sexual exploitation or abuse, whether or not prohibited by law. *Id.* This includes sexual content; erotic, pornographic, or otherwise sexually explicit content; sexually suggestive content, depictions of sexual activity, and fetish content. *Id.* Microsoft also prohibits content that attacks, denigrates, intimidates, degrades, targets, or excludes individuals or groups on the basis of traits such as actual or perceived race, ethnicity, national origin, gender, gender identity, sexual orientation, religious affiliation, age, disability status, caste, or any other characteristic that is associated with systemic prejudice or marginalization. *Id.* Microsoft prohibits content that targets individuals or groups with threats, intimidation, insults, degrading or demeaning language or images, promotion of physical harm, or other abusive behavior such as stalking. *Id.*

In addition to the restrictions and guidelines set forth in customer contracts, the Code of Conduct, the Transparency Note, and Microsoft's AI principles, Microsoft has also developed technical measures controlling access to and enhancing the safety of the Azure OpenAI Service. Lyons Decl. ¶ 19. Microsoft technical measures for protecting the safety of the Azure OpenAI Service include Microsoft's content filtering and abuse detection technologies. *Id.* Within the Azure OpenAI Service, the OpenAI models are integrated with Microsoft-developed content filtering and abuse detection models. *Id.* For example, Azure OpenAI Service includes a content filtering system that works alongside core models, including DALL-E image generation models. *Id.* This system works by running both the prompt and completion through an ensemble of classification models designed to detect and prevent the output of harmful content. *Id.* The content filtering system detects and takes action on specific categories of potentially harmful content in both input prompts and output completions. *Id.* The text content filtering models for

the hate, sexual, violence, and self-harm categories have been specifically trained and tested on the following languages: English, German, Japanese, Spanish, French, Italian, Portuguese, and Chinese. However, the service can work in many other languages. *Id.*

The content filtering system integrated in the Azure OpenAI Service contains Neural multi-class classification models aimed at detecting and filtering harmful content; the models cover four categories (hate, sexual, violence, and self-harm) across four severity levels (safe, low, medium, and high). Lyons Decl. ¶ 20. Other optional classification models are aimed at detecting jailbreak risk and known content for text and code; these models are binary classifiers that flag whether user or model behavior qualifies as a jailbreak attack or match to known text or source code. *Id.*

The Azure OpenAI Service includes default safety applied to all models, with exceptions not relevant here. Lyons Decl. ¶ 21. These configurations provide customers with a responsible experience by default, including content filtering models, blocklists, prompt transformation, content credentials, and others. *Id.* For example, Azure OpenAI DALL-E also comes with prompt transformation by default. *Id.* This transformation occurs on all prompts to enhance the safety of an original prompt, specifically in the risk categories of diversity, deceptive generation of political candidates, depictions of public figures, protected material, and others. *Id.*

In the default streaming scenario, completion content is buffered, the content filtering system runs on the buffered content, and – depending on the content filtering configuration – content is either returned to the user if it doesn't violate the content filtering policy (Microsoft's default or a custom user configuration), or it's immediately blocked and returns a content filtering error, without returning the harmful completion content. Lyons Decl. ¶ 22. This

process is repeated until the end of the stream. *Id.* Content is fully vetted according to the content filtering policy before it's returned to the user. *Id.*

In addition to the content filtering system, Azure OpenAI Service performs Abuse Monitoring to detect content and/or behaviors that suggest use of the service in a manner that might violate applicable product terms. Lyons Decl. ¶ 23. Azure OpenAI Service detects and mitigates instances of recurring content and/or behaviors that suggest use of the service in a manner that may violate the Code of Conduct or other applicable product terms. *Id.*

Microsoft provides access to the Azure OpenAI Service through application programing interfaces, also known as APIs. Lyons Decl. ¶ 24. An API is computer code that enables software applications to communicate with each other. *Id.* Customers who have entered into the necessary contractual agreements with Microsoft may use the Microsoft's APIs to access the Azure OpenAI Service via the Internet using the http protocol. Lyons Decl. ¶ 25. For instance, the example code in Figure 2 below depicts an API call to the Azure OpenAI Service that requests Dall-E to generate an image of Microsoft Clippy wearing a cowboy hat:

Fig. 2

HTTP Copy

```
POST https://{endpoint}/openai/deployments/{deployment-id}/images/generations?api-version=2024-06-01

{
 "prompt": "In the style of WordArt, Microsoft Clippy wearing a cowboy hat.",
 "n": 1,
 "style": "natural",
 "quality": "standard"
}
```

Id. The API-version field tells Microsoft's system what version of the API the customer is using. The "prompt" field is the text description of the desired image, "n" is the number of images

requested, "style" refers to the image style requested, and quality refers to the image resolution (e.g., standard or high definition). Only by communicating in the specific format required by Microsoft's API can a customer access the functionality provided by the Azure OpenAI Service API. Lyons Decl. ¶ 26.

In response to the API call in Figure 2 above, because there is no prohibited content or abuse detected, the Azure OpenAI Service returns a response that includes an image delivery URL. Lyons Decl. ¶¶ 27-28. The "revised_prompt" field indicates the prompt used by the Azure OpenAI Service to generate the image, and the "url" field is the uniform resource locator, e.g., the internet address, of the image generated by the Azure OpenAI Service. *Id.* There is no content filtering called for, so an image is successfully generated and returned to the URL specified in the URL field. By contrast, when the Azure OpenAI Service content filtering system detects harmful content, a user receives either an error on the API call if the prompt was deemed inappropriate, or the finish_reason on the response will be content_filter to signify that some of the completion was filtered. *Id.*

In order to utilize Microsoft APIs to generate an image using DALL-E as described above, a user must authenticate themselves to gain access to the Azure OpenAI Service. Lyons Decl. ¶ 29. The Azure OpenAI Service provides API Key authentication – For this type of authentication, all API requests must include the API Key in the api-key HTTP header. *Id.* An API key is a unique string composed of 52 randomly generated numbers and letters. Lyons Decl. ¶ 30. API keys are used for data plane (content) requests and may be viewed and managed in the customer's Azure Portal. *Id.* Key-based authentication is the default type of authentication for most Azure services. *Id.* For this type of authentication, all API requests must include a valid API key in the api-key HTTP header. *Id.*

Defendants and the Azure Abuse Enterprise

In late July 2024, Microsoft learned that groups of individuals were using stolen Microsoft customer credentials to abuse Microsoft's computers and systems. Microsoft discovered that stolen API keys were being used to generate harmful content in July, 2024, prompting an investigation that revealed the existence of a group of persons who are in the business of using fraud and deception to gain unauthorized access to the Azure OpenAI Service, misusing authentication credentials stolen from paying Microsoft customers, and gaining unauthorized access to and use of Microsoft computers and software for malicious purposes ("The Azure Abuse Enterprise"). Lyons Decl. ¶¶ 5, 33. Defendants collectively manage and use the Azure Abuse Enterprise's technology and services to gain unauthorized access to the Azure OpenAI Service and use generative AI tools to create harmful images that is then distributed to others. Some of these harmful images contain Microsoft's "Azure" trademark in their metadata. Declaration of Maurice Mason in Support of Plaintiff's Motion for Temporary Restraining Order and Related Relief ("Mason Decl.") ¶ 18.

Defendants can be categorized into two distinct groups of actors based on the nature of their conduct. A first group of Defendants is responsible for creating, trafficking, managing, and operating the infrastructure needed to carry out Defendants' attack on the Azure OpenAI Service. This infrastructure includes (i) custom designed client-side software (the de3u application) that allows users to use simple commands to generate malicious images using Microsoft's Azure OpenAI Service APIs; and (ii) custom designed server-side software for trafficking, managing, and operating a reverse proxy service configured with a library of stolen API keys and customer

authentication information. A second group of Defendants is responsible for using the malicious de3u application and reverse proxy service to gain systematic access to Microsoft's systems without authorization and generate harmful images. Together, Defendants conduct this activity as members of the Azure Abuse Enterprise. Lyons Decl. ¶¶ 5-51.

The Azure Abuse Enterprise is responsible for generating several thousand harmful images. The Azure Abuse Enterprise's collective use of stolen customer credentials, customized software tools, and physical infrastructure has allowed Defendants to steal many thousands of dollars' worth of services from Microsoft and its paying customers and to generate thousands of harmful images that have been distributed over the Internet. Lyons Decl. ¶ 7.

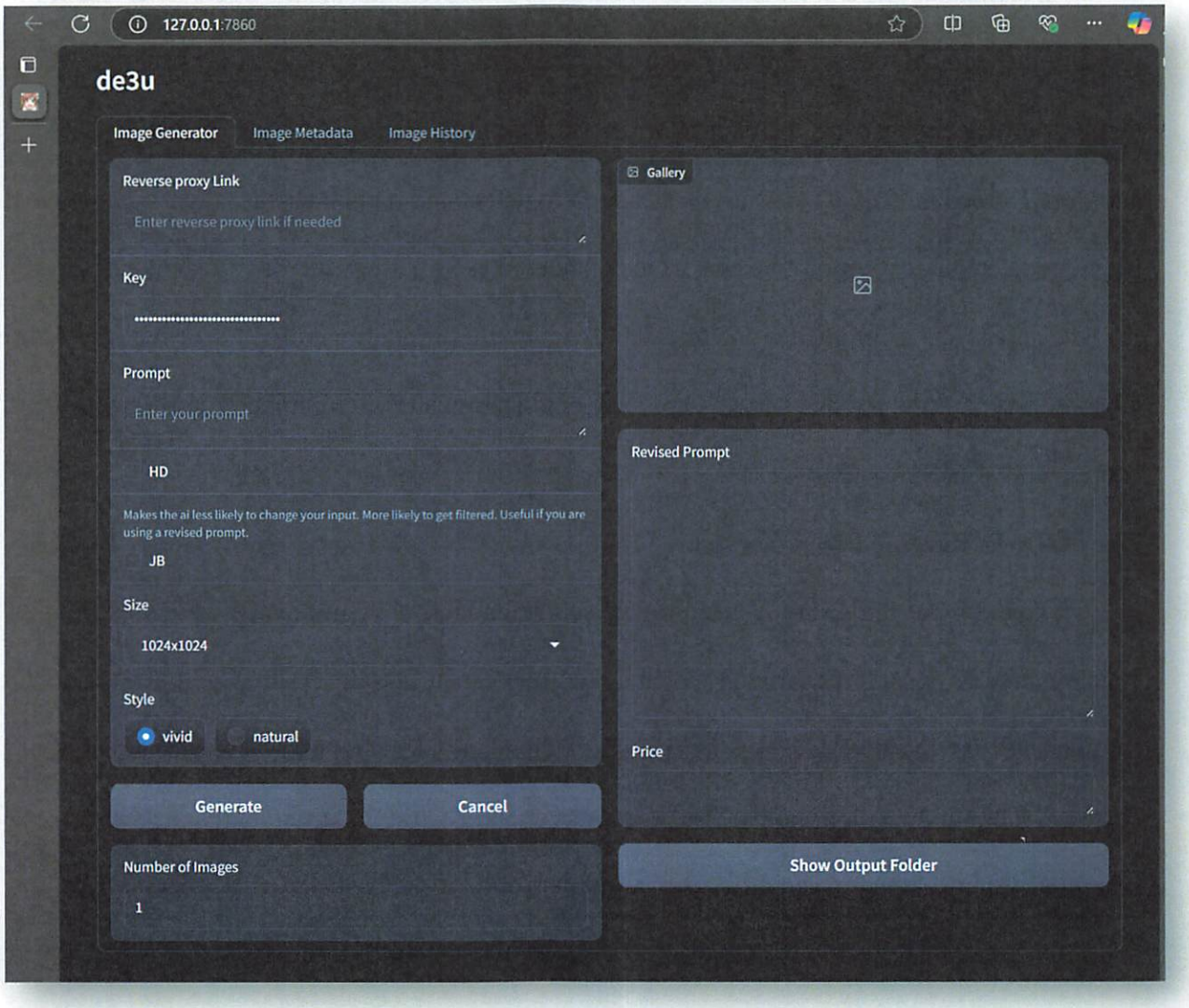
Microsoft acted promptly to investigate and remediate Defendants' conduct, including through cooperation with law enforcement. Although Microsoft has largely remediated the technical exploits Defendants initially leveraged to carry out the Azure Abuse Enterprise, Defendants continue to control stolen API keys, internet infrastructure, and malicious software tools that can be deployed to carry out the illegal conduct described herein. Lyons Decl. ¶ 58.

The de3u Software

The de3u software is designed to grant users unauthorized access to the Azure OpenAI Service and DALL-E image generation model through a simple user interface that leverages Azure APIs. Fiñones Decl.¶ 10. The de3u software translates simple user inputs into Microsoft API calls designed to be authenticated using stolen API keys and other authenticating information. *Id.* For example, by default, the de3u software is hard-coded with a stolen API Key. But a user may direct the de3u software to dynamically request alternative stolen API Keys by electing to direct de3u's API calls to the Azure OpenAI Service, in which case additional technical circumvention occurs at the reverse proxy service level.

Working together with Defendants' reverse proxy service, Defendants' de3u software allows simple mapping of the control fields to input and output parameters so that less sophisticated bad actors can leverage stolen API keys without having to write their own code. Fiñones Decl.¶¶ 10-14. Figure 3 below is a screen capture of the de3u user interface Defendants created:

Fig. 3



Defendants designed their de3u software to be shared with third parties without the need for hosting a web server. Lyons Decl. ¶¶ 38-39. In a web server configuration, users access software that is running on a computer connected to the internet. Defendants' system avoids the need for a web server, relying instead a publicly accessible website, "rentry.org/de3u." Lyons Decl. ¶ 40. This allows Defendants to provide access to their de3u tool—and by extension, access to the Azure OpenAI Service—to anyone in the world who visits that URL. *Id.*

Defendants' de3u software is designed to try to prevent the Azure OpenAI service from revising the original text prompt used to generate images, which can happen for example when a text prompt contains words that trigger Microsoft's content filtering. Lyons Decl. ¶ 41. In addition, Defendants' de3u software is designed to detect and report whether the Azure OpenAI Service rejected a text prompt because it is considered as violating Microsoft's content policy. *Id.* These features, combined with Defendants' unlawful programmatic API access to the Azure OpenAI service, enabled de3u users to reverse engineer means of circumventing Microsoft's content and abuse measures. *Id.*

The "O-A-I" Reverse Proxy Service

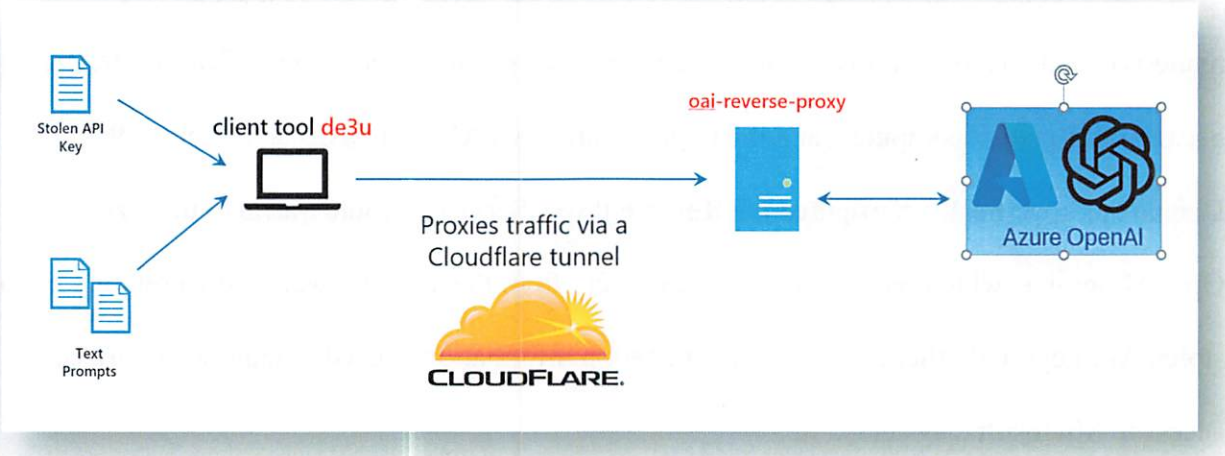
To carry out the Azure Abuse Enterprise, Defendants have implemented and used an "oai" reverse proxy service through which de3u users can access the Azure OpenAI Service ("Reverse Proxy Service"). Lyons Decl. ¶ 47. Defendant's Reverse Proxy Service consists of software running on a physical reverse proxy server and a Cloudflare tunnel that acts as a communications path between de3u user computers and the Azure OpenAI Service. *Id.*

In general, a reverse proxy server is a server that sits in front of web servers and forwards client (e.g. web browser) requests to those web servers. Lyons Decl. ¶ 48. A reverse proxy ensures that no client ever communicates directly with that origin server. *Id.*

In addition to performing the traditional function of any reverse proxy (e.g., forwarding requests), Defendants' oai reverse proxy service processes and alters communications traffic between de3u client computers and the target Azure OpenAI service. Lyons Decl. ¶ 49. Defendants specifically configured the Reverse Proxy Service to route traffic to the Azure OpenAI Service, which reconfigures API calls sent from the de3u software with a rotating list of stolen API keys and other customer authentication information needed to gain unauthorized access to Microsoft's systems. *Id.*

When a de3u user sends a request to the Azure OpenAI service to generate an image, the de3u software routes the request to the Reverse Proxy Service tunnel address. Lyons Decl. ¶ 49. The Reverse Proxy Service parses the request, replaces the original (stolen) hard-coded API key with stolen Azure OpenAI Service API Keys and related authentication information, and then forwards the reconfigured request to the Azure OpenAI Service. *Id.* The request forwarded by the Reverse Proxy Service includes different stolen API keys and associated authentication information based on the stolen API keys and tokens available at the time of the request. *Id.* Figure 4 below depicts de3u communications to the Azure OpenAI service via the Reverse Proxy Service. *Id.*

Fig. 4



The Reverse Proxy Service also receives and processes responses from the Azure OpenAI Service before forwarding responses and other data to the de3u user device. Lyons Decl. ¶ 50. If the de3u user's prompt resulted in generation of an image by the Azure OpenAI service, then the Reverse Proxy Service receives image parameters from the Azure OpenAI service including the URL of the generated image, and the prompt used to generate the image. *Id.* If no image was generated, the Reverse Proxy Service receives and logs the results of any content filtering. *Id.*

If the de3u user's prompt resulted in generation of an image by the Azure OpenAI service, then the Reverse Proxy Service retrieves the image from the URL specified in the Azure OpenAI service return response and saves the image to the computer at an IP address associated with the reverse proxy service ("AWS IP Address"). Lyons Decl. ¶ 51. The Reverse Proxy Service then performs several additional steps including injecting proxy information into the response traffic, setting some HTTP headers, logging events and text prompts, and sending the traffic back to the requesting de3u user client computer. *Id.* Images received by the Reverse Proxy Service from the Azure OpenAI Service include metadata and a unique C2PA Content

Credentials symbol ("CR Icon") identifying Microsoft's Azure OpenAI Service as the technology responsible for generating such images. Mason Decl. ¶ 18.

I. THE COURT HAS JURISDICTION OVER THIS ACTION AND EACH DEFENDANT

The Fourth Circuit has synthesized the due process requirements for specific personal jurisdiction into a three-prong test that considers: "(1) the extent to which the defendant purposefully availed itself of the privilege of conducting activities in the State; (2) whether the plaintiffs' claims arise out of those activities directed at the State; and (3) whether the exercise of personal jurisdiction would be constitutionally reasonable." *Dmarcian, Inc. v. Dmarcian Eur. BV*, 60 F.4th 119, 133 (4th Cir. 2022) (citing *UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344, 352 (4th Cir. 2020)).

Purposeful Availment. The purposeful-availment prong "is not susceptible to a mechanical application" and requires a court to consider "a list of various nonexclusive factors" including:

> 1) whether the defendant maintained offices or agents in the State; (2) whether the defendant maintained property in the State; (3) whether the defendant reached into the State to solicit or initiate business; (4) whether the defendant deliberately engaged in significant or long-term business activities in the State; (5) whether a choice of law clause selects the law of the State; (6) whether the defendant made in-person contact with a resident of the State regarding the business relationship; (7) whether the relevant contracts required performance of duties in the State; and (8) the nature, quality, and extent of the parties' communications about the business being transacted.

Dmarcian, Inc. v. Dmarcian Eur. BV, 60 F.4th 119, 133 (4th Cir. 2022). Here, all applicable purposeful availment factors weigh in favor of jurisdiction.

Although Defendants do not maintain physical offices or human agents within the State, Defendants have effectively set up shop in this Judicial District by choosing websites with top level domains that depend on computers located in Reston, Virginia and a physical AWS IP

Address that geolocates to a physical server located in this State. Lyons Decl. ¶ 56. Sophisticated users of the Internet like Defendants know that ".org" and ".net" TLDs have long been reliant on hardware within Virginia, and by choosing such domains for their malicious infrastructure, Defendants reached into the state to conduct business here. *Id.* Because the enterprise Defendants are carrying out is illegal, there have been no in-person contacts or formal contracts performed within this state, but the performance of Defendants' services is provided through this state at the rentry.org/de3u domain, which serves as the gateway to Defendants' malicious infrastructure. Thus, unlike cases involving passive websites that do nothing more than provide static information to all comers, *see, e.g., Graduate Mgmt. Admission Council v. Raju*, 241 F. Supp. 2d 589, 594 (E.D. Va. 2003), this case involves an interactive website that depends on physical computers located in Virginia in order to receive commands and serve content to end users. For example, when Defendants' malicious Reverse Proxy Service receives harmful images in response to Defendants' use of the de3u software, those images are returned to a computer at the AWS IP address that is physically located in Virginia. Defendants established "continued interaction with their website" infrastructure in Virginia and manifested an intent to carry out their virtual business from within the state. These facts support jurisdiction. *See, e.g., Bright Imperial Ltd. v. RT MediaSolutions, S.R.O.*, Civil Action No. 1:11-cv-935-LO-TRJ, 2012 U.S. Dist. LEXIS 70000, at *23 (E.D. Va. May 18, 2012); *see also Batts v. Snap Inc.*, No. 2:23-cv-03565-DCN, 2024 U.S. Dist. LEXIS 139286, at *18 (D.S.C. July 6, 2024) ("viewed in the context of other jurisdictionally relevant facts…Kurbanov, through his websites, had purposefully availed himself of the privilege of conducting business in Virginia.") (discussing *UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344 (4th Cir. 2020)).

Plaintiffs' Claims Arise from Activities Directed at the State. Plaintiffs' claims all

arise from Defendants' use of the de3u software, Reverse Proxy Service, and AWS IP address to gain unauthorize access to Microsoft's systems and generate images for delivery to and through computers in Virginia. Where affected computers are located within the district, and when Defendants intentional acts cause those computers to effect the harms complained of, jurisdiction is appropriate. See, e.g., *Bright Imperial Ltd.*, 2012 U.S. Dist. LEXIS 70000, at *23; *Batts v. Snap Inc.*, No. 2:23-cv-03565-DCN, 2024 U.S. Dist. LEXIS 139286, at *18 (D.S.C. July 6, 2024); *UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344 (4th Cir. 2020)).

Constitutional Reasonableness. Exercising jurisdiction in Virginia easily satisfies the standard of constitutional reasonableness. "Because [Defendants'] actions were so directly connected to" the rentry.org domain, the AWS IP address, and oai reverse proxy service, all of which are effectively Virginia-based infrastructure, "it is not necessary that [Defendants] step foot in Virginia...so as not to offend the traditional notions of fair play and substantial justice inherent in our Constitution's Due Process Clause." *Bright Imperial Ltd. v. RT MediaSolutions, S.R.O.,* Civil Action No. 1:11-cv-935-LO-TRJ, 2012 U.S. Dist. LEXIS 70000, at *39-40 (E.D. Va. May 18, 2012). "Quite the contrary, it would offend substantial justice to permit" Defendants "to avoid accountability here simply because [they] conducted [their] affairs abroad" in part. *Id.* "It is the ever evolving nature of technology that makes it possible for a foreign defendant to so directly impact the United States…and it would be illogical to permit…individual[s] allegedly responsible for each of the injurious decisions [at issue] to escape the grasps of this Court's judicial authority." *Id.*

National Contacts. "When a defendant's contacts with a single state are insufficient to establish personal jurisdiction within that state, but the defendant's contacts with the United States as a whole are sufficient to establish jurisdiction, any state within the United States may

exercise jurisdiction over the defendant under Rule 4(k)(2)." *Bright Imperial Ltd. v. RT MediaSolutions, S.R.O.*, Civil Action No. 1:11-cv-935-LO-TRJ, 2012 U.S. Dist. LEXIS 70000, at *23-24 (E.D. Va. May 18, 2012). "This Rule permits jurisdiction when (i) a claim arises under federal law, (ii) the defendant is not subject to jurisdiction in any state court, and (iii) exercising jurisdiction does not offend the constitution or laws of the United States." See Fed. R. Civ. P. 4(k)(2). Rule 4(k)(2) is easily satisfied here.

If Defendants are not subject to jurisdiction in Virginia specifically, they are surely subject to jurisdiction in the United States due to their multiple ongoing contacts with the United States as a whole. In addition to their Virginia-based conduct, Defendants intentionally:

- configured their software and systems to use physical machines, technology, and services provided in and from the United States by Microsoft (including, for example, Microsoft Azure servers, technology, and services);
- configured their software and systems to use physical machines, technology, and services provided in and from the United States by Amazon Web Services ("AWS"), a U.S. company;
- configured their software and systems to use physical machines, technology, and services provided in and from the United States by Cloudflare, a U.S. company;
- configured their software and systems to use physical machines, technology, and services provided in and from the United States by PIR,
- configured their software and systems to use physical machines, technology, and services provided in and from the United States by Verisign,
- configured their software and systems to victimize Microsoft, OpenAI, AWS, Cloudflare, PIR, and Verisign
- configured their software and systems to create and distribute harmful images within the U.S:

Lyons Decl. ¶ 57. These sustained and purposeful acts within, towards, and concerning the United States make it constitutionally reasonable for Defendants to be hauled into court here.

"Since such nationwide contacts would satisfy any general personal jurisdiction test, unless inconvenience rises to a level of constitutional concern…minimum contacts with the United States" supports "subjecting [Defendants] to personal jurisdiction" and does not offend the rights protected by the Due Process Clause of the Fifth Amendment. *Noble Sec., Inc. v. MIZ Eng'g, Ltd.*, 611 F. Supp. 2d 513, 553 (E.D. Va. 2009); accord Sunshine Distribution v. Sports Auth. Mich., Inc., 157 F. Supp. 2d 779, 789 (E.D. Mich. 2001) ("This arrangement constitutes 'something more than more awareness that the stream of commerce will sweep the product into the forum state…Instead, Defendant made a deliberate decision" to operate in the U.S.); *Synopsys, Inc. v. Khanh*, No. 22-cv-02546-JD, 2023 U.S. Dist. LEXIS 127044, at *4 (N.D. Cal. July 24, 2023) (national contacts satisfied where piracy website relied on U.S. infrastructure and targeted U.S. software providers).

II. THE RECORD SUPPORTS A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTIVE RELIEF

The fundamental purpose of a preliminary injunction is to prevent irreparable harm during the pendency of a lawsuit and to preserve the court's ability to render a meaningful judgment on the merits. *United States v. South Carolina*, 720 F.3d 518, 524 (4th Cir. 2013) (citations omitted). "Parties seeking a preliminary injunction must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest. *Metro. Reg'l Info. Sys. v. Am. Home Realty Network, Inc.*, 722 F.3d 591, 595 (4th Cir. 2013) (citing *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)).

This matter presents a quintessential case for injunctive relief. Defendants' conduct causes irreparable harm to Microsoft, its customers, and the general public. Every day that passes gives Defendants an opportunity to continue abusing Microsoft's Azure OpenAI Service

and use Microsoft's computers to create harmful content. Unless the requested relief is granted, Defendants will very likely continue to attack generative AI tools provided by Microsoft and/or others, causing irreparable harm.

A. Microsoft Is Likely to Succeed on the Merits of Its Claims

Even at this early stage in the proceedings, the record demonstrates that Microsoft will be able to establish the elements of each of its claims. The evidence in support of Microsoft's TRO application is based on the diligent work of experienced investigators and is supported by substantial empirical evidence and forensic documentation. Given the strength of Microsoft's evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

1. Microsoft's Evidence Shows Defendants' Violations of the CFAA

Congress enacted the CFAA specifically to address computer crime. *See, e.g., Big Rock Sports, LLC v. AcuSport Corp.*, 2011 U.S. Dist. LEXIS 110995, 3 (E.D.N.C. Sept. 26, 2011). "Any computer with Internet access [is] subject [to] the statute's protection." *Id. Inter alia*, the CFAA penalizes a party that intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage. 18 U.S.C. § 1030(a)(5)(C).

A "protected computer" is a computer "used in interstate or foreign commerce or communication." *E.g., SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). In order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000. The CFAA defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Sprint Nextel Corp. v. Simple Cell, Inc.*, 2013 U.S. Dist. LEXIS 99580, 21 (D. Md. July 17,

2013) (citing 18 U.S.C. § 1030(e)(8)). "Damage. . . means any impairment to the integrity or availability of data, a program, a system, or information." *Id.* (citing 18 U.S.C. § 1030(e)(11)). "The Fourth Circuit has recognized that this 'broadly worded provision plainly contemplates consequential damages' such as 'costs incurred as part of the response to a CFAA violation, including the investigation of an offense.'" *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). The CFAA permits plaintiffs to aggregate multiple intrusions or violations for the purpose of meeting the $5,000 statutory threshold. *See Sprint Nextel Corp.*, 2013 U.S. Dist. LEXIS 99580, 21 (citations omitted).

In sum, in order to prevail on their CFAA claim, Microsoft must establish that Defendants (1) accessed a protected computer; (2) without authorization; (3) resulting in loss or damage in excess of $5,000. The Fiñones, Lyons, and Mason Declarations establish that Defendants' conduct satisfies each of these elements. First, the computers that provide the Azure OpenAI Service are protected computers. *See* 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as a computer "used in interstate or foreign commerce or communication"); *see* Lyons Decl. ¶¶ 14-25.

Second, each Azure OpenAI Service computer has been accessed without authorization. API-level access to the Azure OpenAI Service is restricted to customers who have authenticated themselves and received API Keys and other account identifying information from Microsoft. Together, these data elements comprise a digital fingerprint that permits customers to pass through Microsoft's authentication gates for the Azure OpenAI Service. Using stolen credentials to bypass authentication gates is an archetypical example of unauthorized access to computer systems. *See e.g., Microsoft Corp. v. Does*, Civil Action No. 1:22cv607 (LMB/WEF), 2024 U.S. Dist. LEXIS 76088, at *26-27 (E.D. Va. Jan. 10, 2024) (collecting cases including *Global*

Policy Partners, LLC v. Yessin, 686 F. Supp. 2d. 631, 635-38 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA)).

Defendants have engaged in a pattern of systematic API Key theft that enabled them to steal Microsoft Azure OpenAI Service API Keys from multiple Microsoft customers and created a hacking-as-a-service scheme specifically designed to abuse Microsoft's Azure infrastructure and software. Defendants then used the infrastructure to gain unauthorized access to Microsoft's software and computers for the purpose of generating harmful content in violation of Microsoft's policies and technical measures. *See* Statement of Facts p. 3-17, *supra*. This conduct has caused harm to Microsoft exceeding $5,000, including substantial time spent by Microsoft personnel such as Messrs. Lyons, Fiñones, and Mason. Microsoft has also incurred attorneys' fees investigating and bringing this action. The substantial economic and human cost devoted to investigating and remediating Defendants' conduct amounts to well over $5,000 in harm. *See, e.g., GSP Fin. Servs., LLC v. Harrison*, No. GJH-18-2307, 2021 U.S. Dist. LEXIS 16341, at *21 (D. Md. Jan. 28, 2021) ("The Court finds the expenses for legal counsel, cybersecurity consulting, and employees' time are reasonably foreseeable and necessary losses associated with investigating and remedying the harm caused by Defendant's actions.") (citing *Glob. Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 642, 647 (E.D. Va. 2010) and *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009)). The value of the services stolen by Defendants as a result of their CFAA violations also exceeds $5,000.

2. Microsoft's Evidence Shows Defendants' Violations of the DMCA

Section 1201(a)(1) of the DMCA provides that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under [the Copyright Act]." 17 U.S.C. § 1201(a)(1)(A). Like most software, Microsoft's Azure platform consists of software that is entitled to protection under the Copyright Act. Fiñones Decl. ¶¶ 5-7; *e.g.*,

Advanced Comput. Servs. of Mich. v. MAI Sys. Corp., 845 F. Supp. 356, 360 (E.D. Va. 1994) ("software enjoy[s] federal copyright protection").

"A technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3)(B). "To 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." *Id.* § 1201(a)(3)(A).

Microsoft's API Key system is a technological measure that effectively controls access to the Azure Platform, including the Azure OpenAI Service and models that sit behind the service, by requiring the application of API key and customer credential information into HTTP communications sent to the Azure OpenAI Service. Fiñones Decl. ¶¶ 6-19; *see, e.g., Microsoft Corp. v. Pronet Cyber Techs.*, No. 1:08cv434, 2008 U.S. Dist. LEXIS 144931, at *15-16 (E.D. Va. Dec. 5, 2008) ("The record also clearly reflects that defendants trafficked in counterfeit and unauthorized Product Keys and Product Key Labels that are necessarily designed for the purpose of circumventing the technological measure by allowing access to the Microsoft products without proper authorization."); *Apple Inc. v. Psystar Corp.*, 673 F. Supp. 2d 943, 947 (N.D. Cal. 2009) ("lock-and-key" technological measures embedded into software were technological measures for DMCA §1201 purposes).

Defendants' tools alter the ordinary course of operation of Microsoft's API Key system through use of a reverse proxy tool configured with a library of stolen keys and credentials. Fiñones Decl. ¶¶ 6-19; *Philips Med. Sys. Nederland B.V. v. TEC Holdings, Inc.*, No. 3:20-cv-21-MOC-DSC, 2023 U.S. Dist. LEXIS 7319, at *34-35 (W.D.N.C. Jan. 17, 2023) ("Because

Defendants have admitted to using software they developed to bypass Plaintiff's security, there can be no dispute that they have circumvented Plaintiff's technological measures under the plain terms of the DMCA"). Defendants' software and proxy infrastructure are specifically designed to disrupt the ordinary operation of Microsoft's API Key system. For example, when an end user uses de3u to send to the Azure OpenAI service an API call message, the user does not need to include a valid API key or any other customer credentials in their API call message. Instead, the users de3u http message is received at the oai reverse proxy service, which parses the request, alters the message, and appends to it a dynamically selected stolen API key and other identifying information before passing the user's edited HTTP message to the Azure OpenAI Service. Fiñones Decl. ¶¶ 6-19. In such an Azure OpenAI Service attack, the Reverse Proxy Service receives the end user's http communication from the de3u software, checks a library of stolen Azure API keys and associated credentials to find a set of stolen credentials available for use at the moment, and then appends that stolen credential information to the API call, replacing the original API key and altering other portions of the http communication before forwarding that reconfigured http communication to an Azure endpoint. In this way, the de3u end user is able to leverage a library of stolen credentials to bypass the normal operation of Microsoft's API key system so that the end user never has to provide valid authenticating credentials but can instead gain unauthorized access to the Azure OpenAI Service for free. Fiñones Decl. ¶¶ 6-20.

Defendants also used manipulated HTTP commands to bypass Microsoft content filtering controls that would have, in their normal operation, prevented those HTTP commands from being passed through the Azure OpenAI Service for execution by generative AI models. Fiñones Decl. ¶¶ 10-19.

3. Defendants' Conduct Violates the Lanham Act

Defendants' conduct constitutes false designation of origin under section 1125(a), which prohibits use of a registered mark that:

> is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.

15 U.S.C. § 1125(a)(1)(A). Defendants have generated and distributed unauthorized and harmful images containing data identifying Microsoft as the source of such images, C2PA CR Icons identifying the Azure OpenAI Service as the source of the harmful images. Mason Decl. ¶¶ 16-18.

Defendants' malicious images containing C2PA Content Credentials are likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of Defendants and Microsoft, or of Microsoft's sponsorship, or approval of Defendants' goods, services, or commercial activities. This would harm Microsoft's reputation and is likely to dilute by tarnishing Microsoft's famous, distinctive, and widely recognized mark for at least the "Azure" trademark. As such, Defendants' activity is a clear violation of Lanham Act § 1125(a) and Microsoft is likely to succeed on the merits. *See Garden & Gun, LLC v. Twodalgals, LLC*, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *IHOP Corp.*, 2008 U.S. Dist. LEXIS 112056 at *1-3 (same; granting TRO); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a); also constituted trademark "dilution" under §1125(c)); *Brookfield Commc'ns.*, 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie, Inc.*, 1998 U.S. Dist. LEXIS 10729, *12-13 (N.D. Cal.

1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin; also constituted trademark "dilution" under §1125(c)).

4. Defendants' Conduct Violates the RICO Act

Section 1962(c) of the RICO Act provides that:

> It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity or collection of unlawful debt.

18 U.S.C. § 1962(c). Pursuant to this statute, to succeed on a civil RICO claim, "a private RICO plaintiff must allege '(1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity.'" *Field v. GMAC LLC*, 660 F. Supp. 2d 679, 686 (E.D. Va. 2008) (citation omitted). "Racketeering activity" includes any act violative of several specific federal statutes, including 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1029 (access device fraud). 18 U.S.C. § 1961(1). A civil RICO plaintiff must also show that "(5) he was injured in his business or property (6) by reason of the RICO violations." *Borg v. Warren*, 545 F. Supp. 3d 291, 310 (E.D. Va. 2021) (citation omitted).

Defendants are members of an ongoing association-in-fact enterprise. Does 1-3 provide hacking-as-a-service infrastructure. Lyons Decl. ¶ 36. Does 4-5, together with Does 1-3, have used de3u, the oai reverse proxy, stolen API Keys, and maliciously configured HTTP commands to commit wire fraud and access device fraud. Finones Decl. ¶¶ 6-23. The enterprise members function as a continuing unit for the common purpose of achieving the objectives of the enterprise, including the common objectives of wire fraud and access device fraud. Lyons Decl. ¶¶ 5-7.

Defendants have conducted the affairs of the enterprise through a coordinated and

continuous pattern of illegal activity in order to achieve their common unlawful purposes. Does 1-3 each provided funding, devices, infrastructure, resources, and logistical support needed to conduct the enterprise, while Does 4-5 each provided resources, devices, and prompt engineering needed to conduct the enterprise. Defendants have engaged in racketeering by violating the federal wire fraud (18 U.S.C. § 1343) and access device fraud (18 U.S.C. § 1029) statutes.

Wire Fraud (18 U.S.C. § 1343). Defendants have violated the federal wire fraud statute in at least two ways. First, at some point prior to July 2024, Defendants devised a scheme to obtain money or property from Microsoft's paying customers, and to defraud Microsoft, by stealing authentication information from Microsoft customers and misusing that authentication information to access the Azure OpenAI Service. Defendants understood and intended that their misuse of stolen customer authentication information would deplete the account balances of the paying Microsoft customers whose credentials they stole. Defendants devised their scheme at least in part to avoid paying the costs of obtaining a license to the Azure OpenAI Service and purchasing the tokens required to use the Service at scale.[2] *See* Lyons Decl. ¶ 15.

Second, from July 26, 2024 to at least September 17, 2024, Defendants transmitted and/or caused to be transmitted by means of wire communication in interstate and foreign commerce writings, signals, and pictures for the purpose of executing their scheme to defraud. For example, on numerous occasions between July 26, 2024 and August 18, 2024, Defendants transmitted by means of wire communication in interstate and foreign commerce stolen API Key and token information in order to defraud Microsoft regarding Defendants' identities and authorization to access Microsoft's systems and to deprive Microsoft's paying customers of

[2] Tokens refer to the basic units of input and output that the Service processes. Generally, models accessed through the Azure OpenAI Service understand and process text by breaking it down into tokens. Microsoft provides transparent pricing details for input and output tokens at its publicly available website, https://azure.microsoft.com/en-us/pricing/details/cognitive-services/openai-service/.

tokens they had paid for. But for Microsoft's technological remediation efforts, Defendants' conduct would have continued. Defendants continued to use communications transmitted by means of wire communication in interstate and foreign commerce in furtherance of their scheme until at least September 17, 2024, when changes to the oai reverse proxy service were published by one or more of the Defendants.

Access Device Fraud (18 U.S.C. § 1029). Defendants have also violated the access device fraud statute in at least two ways. First, from July 26, 2024 to at least August 18, 2024, Defendants knowingly and with the intent to defraud produced, used, and trafficked in counterfeit access devices including the oai reverse proxy server and de3u computers. Second, from July 26, 2024 to at least August 18, 2024, Defendants knowingly and with intent to defraud trafficked in and used unauthorized access devices, and by such conduct obtained a thing of value aggregating $1,000 or more during that period. Lyons Decl. ¶¶ 5-7.

Defendants' RICO violations caused harm to Microsoft's business and property at least insofar as Defendants have avoided paying the costs of obtaining a license to the Azure OpenAI Service and purchasing the tokens required to use the Service at scale. Id. Given the above, Defendants' activity is a clear violation the RICO Act and Microsoft is likely to succeed on the merits.

5. Defendants' Conduct is Tortious

Defendants' conduct is tortious under the common law doctrines of trespass to chattels and tortious interference. Under Virginia law, the tort of trespass to chattels applies where "personal property of another is used without authorization, but the conversion is not complete." *Dpr Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011) (citations omitted). Here, Defendants used stolen customer information and custom software to gain unauthorized access to Microsoft's Azure OpenAI Service computers, and then exploited that unauthorized access to

create harmful content. District courts in the Fourth Circuit have recognized that similar conduct can amount to tortious conduct under the doctrine trespass to chattels. *See Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 24-25 (E.D. Va. Jan. 6, 2014) ("The unauthorized intrusion into an individual's computer system . . . supports actions under [trespass to chattel claim]"); *see also Microsoft Corp. v. Does*, 2013 U.S. Dist. LEXIS 168237, 3 (W.D.N.C. Nov. 21, 2013) (similar).

Defendants' conduct also amounts to tortious interference. Under Virginia law, the elements of tortious interference with contract are "(1) the existence of a business relationship or expectancy, with a probability of future economic benefit to plaintiff; (2) defendant's knowledge of the relationship or expectancy; (3) a reasonable certainty that absent defendant's intentional misconduct, plaintiff would have continued in the relationship or realized the expectancy; and (4) damage to plaintiff." *Bay Tobacco, LLC v. Bell Quality Tobacco Prod.*, LLC, 261 F. Supp. 2d 483, 500 (E.D. Va. 2003) (citation omitted).

Microsoft has valid contracts with the customers who have been victimized by Defendants. Defendants had knowledge of Microsoft's customer contracts and intentionally set out to wrongfully use Microsoft's customers' contracts and funds for Defendants' own unlawful purposes. In doing so, Defendants have interfered with Microsoft's contracts with its customers by stealing customer account information and using that information to deplete customer account funds. As a result, Defendants' conduct has impeded Microsoft's ability to perform its obligations under its customer contracts.

B. Defendants' Conduct Causes Irreparable Harm

Defendants' conduct causes Microsoft several types of irreparable harm. First, "[n]umerous courts have found that unauthorized access of computers and the acquisition of data in violation of the CFAA constitute irreparable harm." *Chegg, Inc. v. Doe*, No. 22-cv-07326-

CRB, 2023 U.S. Dist. LEXIS 200023, at *21-22 (N.D. Cal. Nov. 7, 2023) (collecting cases). "Several cases within this District have found that fraudulent computer activities cause irreparable harm" under circumstances similar to those presented here. *See Microsoft Corp. v. Does*, Civil Action No. 1:21-cv-822 RDA/IDD, 2022 U.S. Dist. LEXIS 236135, at *11-12 (E.D. Va. Dec. 27, 2022) (citing *Microsoft Corp. v. Peng Yong* et al., Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (injunction to dismantle botnet command and control servers); and *Microsoft v. Piatti,* et al., Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (injunction [*12] to dismantle botnet command and control servers)); *accord Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.) (similar).

Second, loss of the ability to exclude unauthorized persons from accessing Microsoft's copyrightable software irreparably harms Microsoft's anti-circumvention right under the DMCA. *See, e.g., Umg Recordings v. Kurbanov,* Civil Action No. 1:18-cv-957 (CMH/TCB), 2021 U.S. Dist. LEXIS 250844, at *32 (E.D. Va. Dec. 16, 2021) ("Plaintiffs have lost the ability to control how their Works are distributed. Ultimately, this loss of control makes monetary damages inadequate as Defendant's conduct will continue to harm Plaintiffs in the future absent an injunction."); *Synopsys, Inc. v. AzurEngine Techs., Inc.*, 401 F. Supp. 3d 1068, 1074 (S.D. Cal. 2019) (similar, collecting cases).

Third, it is well settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., Int'l Labor Mgmt. Corp. v. Perez*, 2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to "reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief") (citing *In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546 (4th Cir. 1994)); *MicroAire Surgical Instruments, LLC v. Arthrex, Inc.*, 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) ("The loss of

goodwill is a well-recognized basis for finding irreparable harm"). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys. v. Singh*, 2013 U.S. Dist. LEXIS 146938, 9 (D. Md. Oct. 10, 2013); *Nabisco Brands, Inc. v. Conusa Corp.*, 722 F. Supp. 1287, 1290 (M.D.N.C. 1989) ("In the context of a trademark infringement dispute, several courts have held that where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow.").

Here, Defendants' conduct tarnishes Microsoft's valuable trademarks, injuring Microsoft's goodwill, creating confusion as to the source of harmful content created or facilitated by Defendants, and damaging the reputation of Microsoft and the public's confidence in Microsoft's robust safety measures preventing generation and dissemination of harmful content. These injuries are sufficient in and of themselves to constitute irreparable harm.

Lastly, as a practical matter, Defendants are causing harm that is unlikely to ever be compensated by monetary payment—even after final judgment—because Defendants are elusive cybercriminals whom Microsoft is unlikely to be able to enforce judgments against. "[C]ircumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm." *Khepera-Bey v. Santander Consumer USA, Inc.*, 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 2012 Bankr. LEXIS 1107, 9 (Bankr. M.D.N.C. Mar. 15, 2012) ("a preliminary injunction may be appropriate where 'damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered.'"); *Rudolph v. Beacon Indep. Living LLC*, 2012 U.S. Dist. LEXIS 7075, 5 (W.D.N.C. Jan. 23, 2012) ("Irreparable harm exists here because of Defendant Beacon's continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.").

C. The Balance of Equities Strongly Favors Injunctive Relief

Because Defendants are engaged in an illegal scheme to steal from Microsoft's customers in order to obtain unlawful access to Microsoft's systems, circumvent safety mitigations, and create and disseminate harmful content, the balance of equities clearly tips in favor granting an injunction. *See, e.g., US Airways, Inc. v. US Airline Pilots Ass'n*, 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *Pesch v. First City Bank of Dallas*, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Microsoft, its customers, and the public at large, while on the other side rests no legally cognizable harm to Defendants because an injunction would only require them to cease illegal activities. *US Airways*, 13 F. Supp. 2d at 736.

D. The Public Interest Favors an Injunction

It is clear that an injunction would serve the public interest here. The public has a strong interest in enforcing laws like the CFAA, DMCA, and Lanham Act. *See, e.g., BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, 10 (W.D.N.C. Nov. 21, 2008) ("In a trademark case, the public interest is 'most often a synonym for the right of the public not to be deceived or confused.' . . .the infringer's use damages the public interest.") (citation omitted); *accord Meineke Car Care Ctrs., Inc. v. Bica*, 2011 U.S. Dist. LEXIS 118171, 10 (W.D.N.C. Oct. 12, 2011) (similar); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA). The public also has a strong interest in disrupting criminal enterprises operating in violation of the RICO Act. *See, e.g., Amazon.com, Inc. v. WDC Holdings LLC*, Civil Action No. 1:20-cv-484, 2020 U.S. Dist. LEXIS 134555, at *31 (E.D. Va. July 28, 2020) (granting injunction to enjoin RICO enterprise conduct). "Microsoft's proposed injunction is tailored to target and disable communication between Defendants" and to disrupt the malicious infrastructure at issue "with the least amount

of burden on third party domain registries and the public," which ensures that "the public interest would not be harmed, and likely would be served, by a permanent injunction." *Microsoft Corp. v. Doe*, No. 20-CV-1217 (LDH) (RER), 2021 U.S. Dist. LEXIS 101862, at *28 (E.D.N.Y. May 28, 2021)

E. The All Writs Act Authorizes the Court to Direct Third Parties to Perform Acts Necessary to Avoid Frustration of the Requested Relief

Microsoft's Proposed Order directs that the third-party company whose infrastructure Defendants rely on to operate the atism.net domain as part of their hacking-as-a-service scheme reasonably cooperate to effectuate the order. Specifically, Microsoft requests that Verisign take actions to preserve evidence related to the Azure Abuse Enterprise and provide evidence to Microsoft of Defendants' misconduct. Microsoft has received cooperation from ISPs like Verisign under similar circumstances in the past, as most reputable ISPs do not want their infrastructure used to conduct cybercrime.

In addition to the fact that many ISPs will voluntarily comply with orders such as the one Microsoft seeks here, the All Writs Act provides a mechanism for obtaining compliance if needed. The Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). The Supreme Court has recognized that narrow direction to third parties necessary to effect the implementation of a court order is authorized by the All Writs Act:

> The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

United States v. New York Tel. Co., 434 U.S. at 174 (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs

Act); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 30 (E.D. Va. Jan. 6, 2014) (invoking All Writs act and granting relief similar to that requested herein); *United States v. X*, 601 F. Supp. 1039, 1042 (D. Md. 1984) (All Writs Act permits the district court to order a third party to provide "nonburdensome technical assistance" in aid of valid warrant); *Moore v. Tangipahoa Parish Sch. Bd.*, 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power to a federal court to issue such commands . . . as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'") (citing *New York Tel. Co.*, 434 U.S. at 172); *see also In re Application of United States for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of *New York Tel. Co.*, "the Court made the commonsense observation that, without the participation of the telephone company, 'there is no conceivable way in which the surveillance authorized could have been successfully accomplished.'" 434 U.S. at 172); *In re Baldwin-United Corp.*, 770 F.2d 328, 338-339 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction"; "We do not believe that Rule 65 was intended to impose such a limit on the court's authority provided by the All-Writs Act to protect its ability to render a binding judgment."); *Dell Inc.*, 2007 U.S. Dist. LEXIS 98676, at *16 (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

Requiring Verisign to reasonably assist in the execution of the order Microsoft seeks will not offend due process as the Proposed Order (1) requires only minimal assistance from Verisign in executing the order (acts that they would take in the ordinary course of their operations), (2)

requires that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive Verisign of any tangible or significant property interests and (4) requires Microsoft to compensate Verisign for costs, if any, associated with the assistance rendered.

If, in the implementation of the Proposed Order, Verisign wishes to bring an issue to the attention of the Court, Microsoft will bring it immediately. Verisign will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The third party directions in the Proposed Order are thus narrow, satisfy Due Process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless.

F. An *Ex Parte* TRO that Remains Sealed for a Limited Time Is the Only Effective Means of Relief

The Orders Microsoft requests herein must issue *ex parte* for the relief to be effective at all because of the extraordinary factual circumstances here—namely, Defendants' technical sophistication and ability to move their infrastructure and evidence if given advance notice of Microsoft's request for injunctive relief. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers, Lcal No. 70*, 415 U.S. 423, 438-39 (1974) ("*Ex parte* temporary restraining orders are no doubt necessary in certain circumstances[.]").

If notice is given prior to issuance of a TRO, it is likely that Defendants will be able to relocate (or destroy) their infrastructure and associated artifacts before Microsoft can obtain discovery and before the TRO can have any remedial effects. *Ex parte* relief is appropriate under

circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds ...."); *Crosby v. Petromed, Inc.*, 2:09-cv-05055, 2009 U.S. Dist. LEXIS 73419, at *5 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...."); *AT&T Broadband v. Tech Commc'ns, Inc.* 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming ex parte search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Little Tor Auto Center v. Exxon Co.*, U.S.A., 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given"); *Kelly v. Thompson*, 2010 U.S. Dist. LEXIS 31800, *3 (W.D. Tex. Mar. 31, 2010) (granting *ex parte* TRO without notice where irreparable harm would result if notice were given); *In re Vuitton Et Fils S.A.*, 606 F.2d 1, 4-5 (2d Cir. 1979) (per curiam) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless). Courts have previously found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Dell, Inc. v. Belgiumdomains, LLC*, 1:07-cv-22674, 2007 U.S. Dist. Lexis 98676, at *5-6 (S.D. Fla. Nov. 21, 2007).

III. CONCLUSION

For the reasons set forth herein, Microsoft respectfully requests that this Court grant

Microsoft the requested injunctive relief and order this action to remained sealed for a limited period of time necessary to effect the Court's orders.

Dated: December 19, 2024

Respectfully submitted,

JOSHUA CARRIGAN (VA Bar No. 96911)
jcarrigan@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
2100 Pennsylvania Avenue NW
Washington, D.C. 20037
Telephone: + 202 339 8400
Facsimile: + 202 339 8500

ROBERT L. URIARTE (*Pro Hac Vice* forthcoming)
ruriarte@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
355 S. Grand Ave.
Ste. 2700
Los Angeles, CA 90017
Telephone: + 1 213 629 2020
Facsimile: + 1 213 612 2499

JACOB M. HEATH (*Pro Hac Vice* forthcoming)
jheath@orrick.com
ANA M. MENDEZ-VILLAMIL (*Pro Hac Vice* forthcoming)
amendez-villamil@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, CA 94105
Telephone: + 1 415 773 5700
Facsimile: + 1 415 773 5759

LAUREN BARON (*Pro Hac Vice* forthcoming)
lbaron@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
Telephone: + 1 212 506 5000
Facsimile: + 1 212 506 5151

Of Counsel:

RICHARD BOSCOVICH
rbosco@microsoft.com
MICROSOFT CORPORATION
Microsoft Redwest Building C
5600 148th Ave NE
Redmond, Washington 98052
Telephone: +1 425 704 0867
Facsimile: +1 425 706 7329

Attorneys for Plaintiff
MICROSOFT CORPORATION